

BORDER BASIS DETECTION IS NP-COMPLETE

PRABHANJAN V. ANANTH AND AMBEDKAR DUKKIPATI

ABSTRACT. Border basis detection (BBD) is described as follows: given a set of generators of an ideal, decide whether that set of generators is a border basis of the ideal with respect to some order ideal. The motivation for this problem comes from a similar problem related to Gröbner bases termed as Gröbner basis detection (GBD) which was proposed by Gritzmann and Sturmfels (1993). GBD was shown to be NP-hard by Sturmfels and Wiegmann (1996). In this paper, we investigate the computational complexity of BBD and show that it is NP-complete.

1. INTRODUCTION

Gröbner bases play an important role in computational commutative algebra and algebraic geometry as they are used to solve classic problems like ideal membership, intersection and saturation of ideals, solving system of polynomial equations and so on. Gröbner bases are defined with respect to a ‘term order’ and the choice of the term order plays a crucial role in time required to compute Gröbner bases. Gröbner bases are also known to be numerically unstable and hence are not suitable to be used to describe ideals which are constructed from measured data. Border bases, an alternative to Gröbner bases, is known to show more numerical stability as compared to Gröbner bases.

The theory of border bases was used by Auzinger and Stetter [1] to solve zero dimensional polynomial systems of equations. There has been ongoing research to extend this solving technique for solving positive dimensional polynomial systems. The notion of border bases was introduced to find a system of generators for zero dimensional ideals having some nice properties. The theory was generalised to positive dimensional ideals by Chen and Meng [3]. The connection between border bases and statistics was explored by Robbiano, Kruezer and Kehrein [7]. Kehrein and Kreuzer gave characterizations of border bases [5] and also extended Mourrain’s idea [8] to compute border bases [6]. The border bases as computed by the algorithm were associated with degree compatible term orderings. Brian and Pokutta [2]

gave a polyhedral characterisation of order ideals and gave an algorithm to compute border bases which was independent of term orderings. They also showed that computing a preference optimal order ideal is NP-hard.

Gritzmann and Sturmfels [4] introduced Gröbner basis detection (GBD) problem and solved this problem using Minkowski addition of polytopes. Later Sturmfels and Wiegmann [9] showed that GBD is NP-hard. For this, they introduced a related problem called SGBD (Structural Gröbner basis detection) which was shown to be NP-complete by a reduction from the set packing problem. Using SGBD it was proved that GBD is NP-hard. We introduce a similar problem related to border bases known as Border Basis Detection (BBD) and prove that the problem is NP-complete.

In § 2, we give preliminaries for border bases and describe the border basis detection problem. In § 3, we give a polynomial time reduction from 3,4-SAT to BBD and then we will show the correctness of the reduction.

2. BORDER BASES

Let $\mathbb{F}[x_1, \dots, x_n]$ be a polynomial ring, where \mathbb{F} is a field. \mathbb{T}^n denotes the set of terms *i.e.*, $\mathbb{T}^n = \{x_1^{\alpha_1} \dots x_n^{\alpha_n} : (\alpha_1, \dots, \alpha_n) \in \mathbb{Z}_{\geq 0}^n\}$. The total degree of a term $t = x_1^{\alpha_1} \dots x_n^{\alpha_n}$ denoted by $\deg(t)$ is $\sum_{i=1}^n \alpha_i$. We represent all the terms of total degree i by \mathbb{T}_i and all the terms of total degree less than or equal to i by $\mathbb{T}_{\leq i}^n$. By support of a polynomial we mean, all the terms appearing in that polynomial *i.e.*, support of a polynomial $f = \sum_{i=1}^s c_i t_i$, where $c_i \in \mathbb{F}$ and $t_i \in \mathbb{T}^n$ (denoted by $\text{Supp}(f)$) is $\{t_1, \dots, t_s\}$. Similarly, support of a set of polynomials is the union of support of all the polynomials in the set *i.e.*, $\text{Supp}(S) = \bigcup_{f \in S} \text{Supp}(f)$.

The following notions are useful for the theory of border basis.

Definition 1. A non-empty finite set of terms $\mathcal{O} \subset \mathbb{T}^n$ is called an order ideal if it is closed under forming divisors *i.e.*, if $t \in \mathcal{O}$ and $t'|t$ then it implies $t' \in \mathcal{O}$.

Definition 2. Let \mathcal{O} be an order ideal. The border of \mathcal{O} is the set

$$\partial\mathcal{O} = (\mathbb{T}_1^n \cdot \mathcal{O}) \setminus \mathcal{O} = (x_1\mathcal{O} \cup \dots \cup x_n\mathcal{O}) \setminus \mathcal{O}.$$

The first border closure of \mathcal{O} is defined as the set $\mathcal{O} \cup \partial\mathcal{O}$ and it is denoted by $\overline{\partial\mathcal{O}}$.

It can be shown that $\overline{\partial\mathcal{O}}$ is also an order ideal.

Definition 3. Let $\mathcal{O} = \{t_1, \dots, t_\mu\}$ be an order ideal, and let $\partial\mathcal{O} = \{b_1, \dots, b_\nu\}$ be its border. A set of polynomials $G = \{g_1, \dots, g_\nu\}$ is called an \mathcal{O} -border prebasis if the polynomials have the form $g_j = b_j - \sum_{i=1}^{\mu} \alpha_{ij} t_i$, where $\alpha_{ij} \in \mathbb{F}$ for $1 \leq i \leq \mu$ and $1 \leq j \leq \nu$.

Note that the \mathcal{O} -border prebasis consists of polynomials which have exactly one term from $\partial\mathcal{O}$ and rest of the terms are in order ideal \mathcal{O} .

If a \mathcal{O} -border prebasis belongs to an ideal \mathfrak{a} and the order ideal has a nice property with respect to an ideal then that \mathcal{O} -border prebasis is termed as \mathcal{O} -border basis. The definition of \mathcal{O} -border basis is given below.

Definition 4. Let $\mathcal{O} = \{t_1, \dots, t_\mu\}$ be an order ideal and $G = \{g_1, \dots, g_\nu\}$ be an \mathcal{O} -border prebasis consisting of polynomials in \mathfrak{a} . We say that the set G is an **\mathcal{O} -border basis** of \mathfrak{a} if the residue classes of t_1, \dots, t_μ form a \mathbb{F} -vector space basis of $\mathbb{F}[x_1, \dots, x_n]/\mathfrak{a}$.

It can be shown that an \mathcal{O} -border basis of an ideal \mathfrak{a} indeed generates \mathfrak{a} [7]. It can also be shown that for a fixed order ideal \mathcal{O} , with respect to an ideal \mathfrak{a} there can be at most one \mathcal{O} -border basis for \mathfrak{a} . In [5], a criterion was stated for an \mathcal{O} -border prebasis to be \mathcal{O} -border basis termed as “Buchberger criterion for border bases”. The following notion is required for stating that criterion.

Definition 5. Let $G = \{g_1, \dots, g_\nu\}$ be an \mathcal{O} -border prebasis. Two prebasis polynomials g_k, g_l are neighbors, where $k, l \in \{1, \dots, \nu\}$, if their border terms are related according to $x_i b_k = x_j b_l$ or $x_i b_k = b_l$ for some indeterminates x_i, x_j . Then, the corresponding S -polynomials are

$$S(g_k, g_l) = x_i g_k - x_j g_l \text{ and } S(g_k, g_l) = x_i g_k - g_l$$

respectively.

We now state the Buchberger criterion for border bases.

Theorem 2.1. An \mathcal{O} -border prebasis $G = \{g_1, \dots, g_\nu\}$ is an \mathcal{O} -border basis of an ideal \mathfrak{a} if and only if $G \subset \mathfrak{a}$ and, for each pair of neighboring prebasis polynomials g_k, g_l , there are constant coefficients $c_j \in \mathbb{F}$ such that

$$S(g_k, g_l) = c_1 g_1 + \dots + c_\nu g_\nu.$$

The proof for the above theorem can be found in [5]. In the next section, we state BBD and give our result.

3. RESULT

BBD is described as follows:

Given a set of polynomials \mathcal{F} such that $\mathfrak{a} = \langle \mathcal{F} \rangle$ where \mathfrak{a} is an ideal, decide whether \mathcal{F} is a \mathcal{O} -border basis of \mathfrak{a} for some order ideal \mathcal{O} .

We first describe the input representation of the polynomials for the BBD instance. We follow the “sparse representation” as in [4] to represent the polynomials in \mathcal{F} . Let $\mathbb{F}[x_1, \dots, x_n]$ be the polynomial ring under consideration and let \mathcal{F} be the set of input polynomials in the BBD instance. Consider a polynomial $f = c_1 X^{\alpha_1} + \dots + c_s X^{\alpha_s} \in \mathcal{F}$ where $c_i \in \mathbb{F}$, $X^{\alpha_i} = x_1^{\alpha_{1i}} \dots x_n^{\alpha_{ni}}$ for $i \in \{1, \dots, s\}$ and $\alpha_i = (\alpha_{1i}, \dots, \alpha_{ni}) \in \mathbb{Z}_{\geq 0}^n$. f is represented by its nonzero field coefficients c_1, \dots, c_k and its corresponding nonnegative exponent vectors $\alpha_1, \dots, \alpha_s$.

In this section, we show that BBD is NP-complete. The NP-complete problem we have chosen for our reduction is 3,4-SAT. 3,4-SAT denotes the class of instances of the satisfiability problem with exactly three variables per clause and each variable or its complement appears in no more than four clauses. The 3,4-SAT problem was shown to be NP-complete by Tovey [10].

Let \mathcal{I} be an instance for the 3,4-SAT problem. Let X_1, \dots, X_n be variables and C_1, \dots, C_m be clauses in \mathcal{I} such that $\mathcal{I} = C_1 \wedge C_2 \dots \wedge C_m$. Each clause is a disjunction of three literals. For example, $(X_i \vee \overline{X}_j \vee X_k)$ represents a clause for $i, j, k \in \{1, \dots, n\}$. Assume without loss of generality that X_i appears in at least one clause and so does \overline{X}_i . Also assume that X_i and \overline{X}_i do not appear in the same clause for any $i \in \{1, \dots, n\}$. We construct a BBD instance from this 3,4-SAT instance.

Consider the polynomial ring

$$P = \mathbb{F}[x_1, \dots, x_n, \overline{x}_1, \dots, \overline{x}_n, c_1, \dots, c_m, x_{c_1}, \dots, x_{c_m}, X],$$

where \mathbb{F} is a field. We will reduce the 3,4-SAT instance \mathcal{I} to a set of polynomials $\mathcal{F} \subset P$. Note that P is a polynomial ring with $N = 2n + 2m + 1$ indeterminates. Before we describe the reduction, we list some definitions and observations that will be useful for our reduction.

- With respect to all the clauses in which X_i, \overline{X}_i appear for $i \in \{1, \dots, n\}$, we associate the term $t_{C_{x_i}} = \left(\prod_{j \in S} c_j \right) X^\alpha$ where for each $j \in S \subset \{1, \dots, m\}$ either X_i or \overline{X}_i appears in C_j and $\alpha = 4 - |S|$. Note that $\deg(t_{C_{x_i}}) = 4$.

- With respect to each X_i, \overline{X}_i for $i \in \{1, \dots, n\}$, we associate the terms $t_{X_i} = x_i \overline{x}_i^2 t_{C_{x_i}}$, $t_{\overline{X}_i} = x_i^2 \overline{x}_i t_{C_{x_i}}$ respectively. Note that $\deg(t_{X_i}) = \deg(t_{\overline{X}_i}) = 7$.
- We define children of a term t to be

$$k(t) = \{t' \mid \text{for some indeterminate } y, t'y = t\}.$$

Note that each term can have at most N children.

- Extending the above definition, we define children of a set of terms S to be $k(S) = \bigcup_{t \in S} k(t)$. It follows that for two sets of terms A and B , $k(A \cup B) = k(A) \cup k(B)$.
- We define parents of a term t to be

$$p(t) = \{t' \mid \text{for some indeterminate } y, ty = t'\}.$$

Note that each term has exactly N parents.

- Extending the above definition, we define parents of a set of terms S to be $p(S) = \bigcup_{t \in S} p(t)$.
- $K_{X_i} = \left\{ \frac{t_{X_i} x_{c_l}}{c_l} \mid X_i \text{ appears in clause } C_l \text{ for some } l \in \{1, \dots, m\} \right\}$ for $i = 1, \dots, n$.
- $K_{\overline{X}_i} = \left\{ \frac{t_{\overline{X}_i} x_{c_l}}{c_l} \mid \overline{X}_i \text{ appears in clause } C_l \text{ for some } l \in \{1, \dots, m\} \right\}$ for $i = 1, \dots, n$.
- $K_i = K_{X_i} \cup K_{\overline{X}_i} \cup \{t_{X_i}, t_{\overline{X}_i}\}$ for $i = 1, \dots, n$.
- $P_{X_i} = \left\{ t_{X_i} x_{c_l} \mid X_i \text{ appears in clause } C_l \text{ for some } l \in \{1, \dots, m\} \right\}$ for $i = 1, \dots, n$.
- $P_{\overline{X}_i} = \left\{ t_{\overline{X}_i} x_{c_l} \mid \overline{X}_i \text{ appears in clause } C_l \text{ for some } l \in \{1, \dots, m\} \right\}$ for $i = 1, \dots, n$.
- $P_i = P_{X_i} \cup P_{\overline{X}_i}$ for $i = 1, \dots, n$. The number of clauses X_i or \overline{X}_i appear is $|P_i|$. Hence, $|P_i| \leq 4$.
- We define $I(t)$ to be the number of indeterminates that divide a term t . Note that $I(t) = k(t)$.
- Region associated with X_i, \overline{X}_i for $i \in \{1, \dots, n\}$ is defined as

$$R_i = k(P_i) = k(P_{X_i}) \cup k(P_{\overline{X}_i}).$$

In other words R_i consists of all the children of P_i and hence $|R_i| \leq 4N$. For $i, j \in \{1, \dots, n\}$ and $i \neq j$, since every term in R_i contains either x_i or \overline{x}_i (and does not contain x_j, \overline{x}_j) and

*This notation is used for convinience. If t', t are terms such that $t'x = t$ for some indeterminate x then we represent t' as $\frac{t}{x}$.

similarly every term in R_j contains either x_j or \bar{x}_j (and does not contain x_i, \bar{x}_i) and hence $R_i \cap R_j = \phi$.

- For a set $S \subset \mathbb{T}^n$, we define $\maxdeg(S)$ to be $\max_{t \in S} \{deg(t)\}$ i.e. \maxdeg is a function from power set of \mathbb{T}^n to \mathbb{N} which associates to each set $S \subset \mathbb{T}^n$ a number n such that there exists a term in S having total degree n and no term in S has total degree greater than n .

We now state and prove a few observations that will be used for the reduction.

Lemma 3.1. *Two distinct terms can have no more than one common parent i.e., for two distinct terms t_1, t_2 , $|p(t_1) \cap p(t_2)| \leq 1$.*

Proof. Consider two terms t_1, t_2 such that $t_1 \neq t_2$. Assume that there exists two distinct terms t, t' such that $t_1, t_2 \in k(t)$ and $t_1, t_2 \in k(t')$. This implies that there exists indeterminates y_1, y_2, y'_1, y'_2 such that

$$t_1 y_1 = t, \quad t_2 y_2 = t, \quad t_1 y'_1 = t', \quad t_2 y'_2 = t'.$$

This implies that $y'_2 y_1 = y'_1 y_2$. Since, $y_1 \neq y'_1$ and $y_1 \neq y_2$, we get a contradiction. \square

Corollary 3.2. *For two distinct terms t_1, t_2 , $|k(t_1) \cap k(t_2)| \leq 1$.*

Proof. This follows from the definition and the previous lemma. \square

Corollary 3.3. *Let S be a set of terms and t be a term such that $t \notin S$. Then $|k(t) \cap k(S)| \leq |S|$.*

Proof. Let $S = \bigcup_{i: a_i \in S} \{a_i\}$. We have

$$k(t) \cap k(S) = \bigcup_{i: a_i \in S} (k(t) \cap k(a_i)).$$

But,

$$\begin{aligned} \left| \bigcup_{i: a_i \in S} (k(t) \cap k(a_i)) \right| &\leq \sum_{i: a_i \in S} |k(t) \cap k(a_i)| \\ &\leq |S| \text{ (from the previous corollary).} \end{aligned}$$

Hence, $|k(t) \cap k(S)| \leq |S|$. \square

Lemma 3.4. *No two terms from two different regions can have a common parent i.e., if there are two terms $t_1 \in R_i$, $t_2 \in R_j$ then there exists no term t_3 such that $t_1, t_2 \in k(t_3)$.*

Proof. Let $t_1 \in R_i$ and $t_2 \in R_j$ for some $i, j \in \{1, \dots, n\}$. Assume without loss of generality that $t_1 \in k(t_{X_i}y)$ (a similar argument holds if $t_1 \in k(t_{\overline{X}_i}y)$), where y is an indeterminate such that $t_{X_i}y \in P_{X_i}$. Hence, there exists an indeterminate y' such that $t_1y' = t_{X_i}y$. Now, if we assume that there exists a term t_3 such that $t_1, t_2 \in k(t_3)$ then there exists two indeterminates y_1, y_2 such that,

$$t_3 = t_1y_1 = t_2y_2 \Rightarrow t_{X_i}yy_1 = t_2y_2y'.$$

But, $x_i\overline{x}_i^2|t_{X_i} \Rightarrow x_i\overline{x}_i^2|t_2y_2y' \Rightarrow x_i\overline{x}_i^2|y_2y'$ (since x_i, \overline{x}_i does not divide any term in R_j) and hence a contradiction. \square

Lemma 3.5. *Let \mathcal{O} be an order ideal. If all the children of a term t are in $\partial\mathcal{O}$ then t cannot be in $\partial\mathcal{O}$ and \mathcal{O} i.e., for a term t such that $k(t) \subset \partial\mathcal{O}$ then $t \notin \mathcal{O}, t \notin \partial\mathcal{O}$.*

Proof. Let t be a term such that $k(t) \subset \partial\mathcal{O}$. If $t \in \mathcal{O}$ then $k(t) \subset \mathcal{O}$ and hence $t \notin \mathcal{O}$. If $t \in \partial\mathcal{O}$ then there exists some indeterminate y' such that for some term $t' \in \mathcal{O}$, we have $t'y' = t$. But $t' \in k(t) \Rightarrow t' \in \partial\mathcal{O}$, a contradiction. Hence, $t \notin \partial\mathcal{O}$. \square

Lemma 3.6. *For a term t such that $t \in k(P_i)$ where $i \in \{1, \dots, n\}$, then $I(t) \geq |P_i| + 2$.*

Proof. For a term $t' \in P_i$, $I(t') = 3 + I(t_{C_{x_i}})$, but

$$\begin{aligned} I(t_{C_{x_i}}) &= \min(\text{number of clauses in which } X_i, \overline{X}_i \text{ appear} + 1, 4) \\ &= \min(|P_i| + 1, 4). \end{aligned}$$

We have $I(t') = \min(|P_i| + 1, 4) + 3$ and thus for $t \in k(t')$,

$$I(t) \geq \min(|P_i| + 1, 4) + 2 = \min(|P_i| + 3, 6) \text{ and since } |P_i| \leq 4,$$

$$I(t) \geq |P_i| + 2.$$

\square

Lemma 3.7. *Let t_1, t_2 be terms such that $t_1t = t_2$ where t is a term and $t \neq 1$. If x is an indeterminate such that x divides t then $t_1 \left| \frac{t_2}{x} \right.$.*

Proof. Since x divides t , x also divides t_2 and hence $\frac{t_2}{x}, \frac{t}{x}$ are valid terms. We have, $t_1\left(\frac{t}{x}\right) = \frac{t_2}{x}$. Thus, $t_1 \left| \frac{t_2}{x} \right.$. \square

In other words, the above lemma states that if a term t_1 divides t_2 and $t_1 \neq t_2$, then there exists a child of t_2 , say t_3 such that t_1 divides t_3 .

3.1. BBD is in NP. We ask the following question: When does a set of terms be a border with respect to an order ideal. It turns out that if the terms in B obey some conditions then there exists an order ideal such that B is its border.

Let $B \subset \mathbb{T}^n$ be a finite set of terms. Let B' be a subset of B such that every term t in B' obeys the following conditions:

- 1) For indeterminates y, x such that $x|t$ and $y \neq x$, atleast one of $ty, \frac{ty}{x}, \frac{t}{x}$ is in B .
- 2) There exists an indeterminate x such that $x|t$ and $\frac{t}{x} \notin B$.
- 3) Let t', t'' be terms such that $t'|t'', t''|t$ and t'' is the parent of t' . If $t' \in B$ then t'' is in B .

If $B = B'$ then we say that “ B satisfies the three conditions” else we say that “ B does not satisfy the three conditions”. We will later prove that the three conditions mentioned before are sufficient and necessary for the existence of an order ideal such that B is its border. Before that we state an equivalent formulation of third condition.

For a term t in B consider the following set:

$$S_t = \left\{ t'' \in \mathbb{T}^n \mid t''|t \text{ and } \exists \text{ a term } t' \in B \text{ such that } t'|t'' \right\}$$

Lemma 3.8. *All the terms in B obey the third condition if and only if $S_t \subset B$ for all $t \in B$.*

Proof. If for all $t \in B$, $S_t \subset B$ then B satisfies the third condition.

Assume all terms in B obey the third condition. Let t be a term in B and let S'_t be the subset of S_t such that it contains all the terms in S_t and not in B . If $S'_t = \emptyset$ then $S_t \subset B$. Hence assume that $S'_t \neq \emptyset$. Let t'' be a term in S'_t such that no term in S'_t divides t'' . Since $t'' \in S_t$, there exists a term t_1 such that $t_1|t''$ and $t_1 \in B$. From lemma 3.7, $t_1|t'$ where $t' \in k(t'')$. Since $t_1|t', t'|t$ and $t_1 \in B$, we have $t' \in S_t$. By the choice of t'' , $t' \in S'_t$ which means $t' \in B$. We have a situation where there are three terms t, t', t'' such that (i) $t'|t'', t''|t$, (ii) $t, t' \in B$, $t'' \notin B$ and (iii) $t'' \in p(t')$. But this contradicts the fact that all the terms in B satisfy the third condition. \square

From the above lemma, for a term $t \in B$ the third condition can be rephrased as follows:

- 3a) For terms t', t'' such that $t' \in B$, $t'|t''$ and $t''|t$ then t'' is in B .

We now give the necessary and sufficient conditions for B to be the border of an order ideal \mathcal{O} .

Theorem 3.9. *There exists an order ideal \mathcal{O} such that $\partial\mathcal{O} = B$ if and only if B satisfies all the conditions.*

Proof. Let \mathcal{O} be an order ideal such that B is its border i.e. $B = \partial\mathcal{O}$. Assume that B does not satisfy the three conditions which means there exists a term $t \in B$ which does not obey all the three conditions. Consider the following cases:

Case (i) Suppose t does not obey the first condition. There exists indeterminates x, y such that $x|t, y \neq x$ and $t_1 = ty \notin B, t_2 = \frac{ty}{x} \notin B, t_3 = \frac{t}{x} \notin B$. Since $t \in \partial\mathcal{O}$, t_3 is in \mathcal{O} which implies that $t_3y = t_2 \in \mathcal{O}$ since $t_2 \notin \partial\mathcal{O}$. Similarly, $t_2x = t_1 \in \mathcal{O}$. But \mathcal{O} is an order ideal and since $t|t_1$, t should be in \mathcal{O} and hence a contradiction.

Case (ii) Suppose t does not obey the second condition. Then $k(t) \subset B = \partial\mathcal{O}$. From lemma 3.5, $t \notin \partial\mathcal{O}$ which is a contradiction.

Case (iii) Suppose t does not obey the third condition. There exists two terms t', t'' such that $t' \in B, t'' \in \mathcal{O}$ and $t'|t'', t''|t, t'' \in p(t')$. Since \mathcal{O} is an order ideal, $t'' \in \mathcal{O}$ implies that $t' \in \mathcal{O}$, a contradiction.

Hence B has to satisfy the three conditions for it to be the border of the order ideal \mathcal{O} .

Assume that B satisfies all the three conditions. Now, consider the following set:

$$\mathcal{O} = \left\{ t \in \mathbb{T}^n \mid \text{there exists a term } t' \in B \text{ such that } t|t' \text{ and } t \notin B \right\}$$

Claim. \mathcal{O} is an order ideal.

Proof. Consider a term $t \in \mathcal{O}$. Let t' be a term such that $t'|t$. By the construction of \mathcal{O} , there exists a term $t'' \in B$ such that $t|t''$ and this implies that $t'|t''$. Now, if t' was in B then from lemma 3.8, t'' would violate the third condition and hence $t' \notin B$. Hence, $t' \in \mathcal{O}$.

Claim. $B = \partial\mathcal{O}$.

Proof. We will first show that $B \subset \partial\mathcal{O}$. Consider a term $t \in B$ and from the second condition there exists a term $t' \notin B$ such that $t = t'x$ for some indeterminate x . This implies that $t' \in \mathcal{O}$ and hence, $t'x = t \in \partial\mathcal{O}$ since $t \notin \mathcal{O}$. It remains to show that $\partial\mathcal{O} \subset B$. Let $t_1 \in \partial\mathcal{O}$ and hence there exists a term $t \in \mathcal{O}$ such that $tx = t_1 \in \partial\mathcal{O}$ for an indeterminate x . From the construction of \mathcal{O} , t divides at least one term in B . Let $t_2 \in B$ such that $t|t_2$ and if there is a term t' such that $t|t'$ and $t'|t_2$ then $t' \in \mathcal{O}$. Since $t|t_2$, from lemma 3.7 there exists a child of t_2 such that t divides that term. Let x_1 be an indeterminate such that $x_1|t_2$ and $t|\frac{t_2}{x_1}$. Consider the following two cases:

Case (i) $x_1 = x$: In this case $t_1|t_2$ and hence $t_1 \in B$ since $t_1 \notin \mathcal{O}$.

Case (ii) $x_1 \neq x$: From the first condition, one of $t_2x, \frac{t_2x}{x_1}, \frac{t_2}{x_1}$ has to be in B . Assume that $\frac{t_2}{x_1} \in B$. We have a term $t_2'' = \frac{t_2}{x_1}$ such that $t|t_2'', t_2''|t_2$

and $t_2'' \in B$ which contradicts the choice of t_2 . Hence $\frac{t_2}{x_1} \notin B$ which means $\frac{t_2 x}{x_1}$ or $t_2 x$ is in B . Now $t \mid \left(\frac{t_2}{x_1}\right)$ and hence $tx \mid \left(\frac{t_2 x}{x_1}\right)$, $tx \mid t_2 x$ which implies that $tx = t_1$ divides a term in B . This further implies that $t_1 \in \mathcal{O}$ or $t_1 \in B$. Since $t_1 \in \partial\mathcal{O}$, $t_1 \notin \mathcal{O}$ and thus $t_1 \in B$. \square

Let B be a set of terms and let m be the size of binary representation of B .

For a term $t \in B$ and a fixed pair of indeterminates (y, x) , we can search whether $\frac{ty}{x}, \frac{t}{x}, ty$ are in B in $O(m)^\dagger$ time. And since there are $|B|(\leq m)$ terms and N^2 pairs of indeterminates (N is the number of indeterminates), condition 1 can be checked in $O(m^2 N^2)$ time.

For every term t , atmost N children are possible. In $O(Nm)$ time it can be checked whether all the children of the term t are in B or not. Since there are $|B|$ terms, condition 2 can be checked in $O(Nm^2)$ time. Every term has exactly N parents. For terms $t', t'' \in B$ fixed such that $t' \mid t$, it takes $O(Nm)$ time to check whether all the parents of t' dividing t are in B . Since there are $|B|^2$ such terms possible, condition 3 can be checked in $O(Nm^3)$ time.

Hence, it can be checked in time polynomial in N and m (binary size of B) whether B is the border of some order ideal.

Let B be the border of some order ideal \mathcal{O} i.e. $B = \partial\mathcal{O}$ and let \mathcal{F} be a set of polynomials such that the support of each polynomial in \mathcal{F} contains exactly one term from B and $|B| = |\mathcal{F}|$. We state a lemma that will be helpful in checking whether \mathcal{F} is a \mathcal{O} -border prebasis.

Lemma 3.10. *\mathcal{F} is a \mathcal{O} -border prebasis if and only if every term in $\text{Supp}(\mathcal{F}) \setminus B$ divides a term in B .*

Proof. Let \mathcal{F} be a \mathcal{O} -border prebasis. Then $B' = \text{Supp}(\mathcal{F} \setminus B) \subset \mathcal{O}$. Let $t \in B'$ i.e. $t \in \mathcal{O}$. For an indeterminate x , consider the sequence of terms t, tx, tx^2, \dots . Not all the terms in the sequence can be in \mathcal{O} since \mathcal{O} is a finite set of terms. Let i be the least number such that $tx^i \notin \mathcal{O}$ and hence $tx^i \in \partial\mathcal{O}$. Thus, t divides a term in $\partial\mathcal{O}$.

Let t be a term in B' such that t divides a term $t' \in B$. As mentioned before, $\partial\mathcal{O}$ is an order ideal and hence $t \in \partial\mathcal{O}$. Since, $t \notin \partial\mathcal{O}$, t has to be in \mathcal{O} . Thus, $B' \subset \mathcal{O}$. Hence, $|B| = |\mathcal{F}|$ and support of each polynomial in \mathcal{F} contains exactly one term in B and the rest of the terms are in \mathcal{O} . Thus, \mathcal{F} is a \mathcal{O} -border prebasis. \square

We now give the proof that BBD is in NP.

[†]Big-O notation

Theorem 3.11. *BBD is in NP.*

Proof. Let \mathcal{F} be a set of input polynomials to the BBD instance such that $\mathfrak{a} = \langle \mathcal{F} \rangle$. Assume that a set $B = \text{Supp}(\mathcal{F})$ containing exactly one term from each polynomial in \mathcal{F} and $|B| = |\mathcal{F}|$, is given as a “YES” certificate[‡] for \mathcal{F} such that $B = \partial\mathcal{O}$ for some order ideal \mathcal{O} and \mathcal{F} is a \mathcal{O} -border basis. Let the binary size of representation of \mathcal{F}, B be denoted by $m_{\mathcal{F}}, m_B$ respectively. This certificate can be verified in polynomial time as follows:

We have seen that it can be verified in time polynomial in m_B and N whether B is the border of some order ideal \mathcal{O} . In order to check whether \mathcal{F} is a \mathcal{O} -border prebasis, from the previous claim we need to check whether each term in $\text{Supp}(\mathcal{F}) \setminus B$ divides a term in B . This can be implemented in $O(m_{\mathcal{F}}m_B)$ time. And in time polynomial in $m_{\mathcal{F}}$, it can be verified whether \mathcal{F} satisfies the Buchberger criterion. Since a “YES” certificate for the BBD instance can be verified in polynomial time, BBD is in NP. \square

We now give a polynomial time reduction from 3,4-SAT to BBD.

3.2. Reduction. We are now going to construct a set of polynomials \mathcal{F} as follows:

- With respect to variable X_i for $i \in \{1, \dots, n\}$, associate a polynomial

$$t_{X_i} + t_{\overline{X}_i}.$$

We shall refer to such polynomials as ***v-polynomials*** (variable polynomials)

$$F_v = \{t_{X_i} + t_{\overline{X}_i} \mid i = 1, \dots, n\}.$$

i.e F_v is a set of *v-polynomials*.

- With respect to each clause C_l in \mathcal{I} for $l \in \{1, \dots, m\}$, we associate a polynomial. Without loss of generality assume that $C_l = (X_i \vee \overline{X}_j \vee X_k)$, for $i, j, k \in \{1, \dots, n\}$. The polynomial associated with C_l is

$$\frac{t_{X_i}x_{c_l}}{c_l} + \frac{t_{\overline{X}_j}x_{c_l}}{c_l} + \frac{t_{X_k}x_{c_l}}{c_l}.$$

We will refer to the above set of polynomials as ***c-polynomials***

[‡]A “YES” certificate is a proof to show that \mathcal{F} corresponds to an “yes” answer in BBD i.e. \mathcal{F} is a border basis of \mathfrak{a} with respect to some order ideal.

(clause polynomials).

$$F_c = \left\{ \frac{t_{X_i}x_{c_l}}{c_l} + \frac{t_{X_j}x_{c_l}}{c_l} + \frac{t_{X_k}x_{c_l}}{c_l} \mid C_l = (X_i \vee X_j \vee X_k) \text{ is a clause in } \mathcal{I} \right\}$$

- The third set of polynomials are those that contain just one term in their support:

$$F_1 = \{t \mid \deg(t) = 8\}, F_2 = \bigcup_{i=1}^n (R_i \setminus K_i), \mathcal{F}' = F_1 \cup F_2.$$

We refer to the set of polynomials in \mathcal{F}' as **t -polynomials** (polynomials containing just one term).

From the above set of polynomials, we construct the system of polynomials \mathcal{F} which is an instance to the BBD problem:

$$\mathcal{F} = F_v \cup F_c \cup \mathcal{F}'.$$

Note that all the terms in $\text{Supp}(\mathcal{F})$ have total degree either 7 or 8. Also, for any two polynomials $f, g \in \mathcal{F}$ we have $\text{Supp}(f) \cap \text{Supp}(g) = \emptyset$.

The construction of each polynomial in F_c, F_v can be done in time polynomial in n, m . So F_c, F_v can be constructed in time polynomial in n and m since $|F_c| = m$ and $|F_v| = n$. F_1, F_2 can be computed in time polynomial in $|F_1|$ and $|F_2|$. Also $|F_2|$ is bounded above by $\sum_{i=1}^n |R_i|$ ($\leq \sum_{i=1}^n 4N \leq 4nN$) and $|F_1| \leq \binom{8+N}{8} < N^8$. Hence F_1, F_2 can be constructed in time polynomial in N . Since F_c, F_v, F_1 and F_2 can be constructed in time polynomial in N , the reduction can be performed in polynomial time.

We state a theorem that will be helpful for proving the correctness of reduction in the next section.

Theorem 3.12. *Let \mathcal{F} be a \mathcal{O} -border basis. If X_i appears in C_l for $i \in \{1, \dots, n\}$, $l \in \{1, \dots, m\}$ then both t_{X_i} and $\frac{t_{X_i}x_{c_l}}{c_l}$ cannot be in $\partial\mathcal{O}$. Similarly if \overline{X}_i appears in C_l for $i \in \{1, \dots, n\}$, $l \in \{1, \dots, m\}$, then both $t_{\overline{X}_i}$ and $\frac{t_{\overline{X}_i}x_{c_l}}{c_l}$ cannot be in $\partial\mathcal{O}$.*

Proof. Assume that X_i appears in C_l . We have

$$k(t_{X_i}x_{c_l}) \cap \text{Supp}(F_c \cup F_v) = \left\{ t_{X_i}, \frac{t_{X_i}x_{c_l}}{c_l} \right\} \text{ and}$$

$$k(t_{X_i}x_{c_l}) \setminus \left\{ t_{X_i}, \frac{t_{X_i}x_{c_l}}{c_l} \right\} \subset F_2 .$$

Since F_2 contains t -polynomials, every term in the support of F_2 has to be in $\partial\mathcal{O}$ and similarly all the terms in F_1 has to be in $\partial\mathcal{O}$. Hence,

$$t_{X_i}x_{c_l} \in \partial\mathcal{O}, \quad k(t_{X_i}x_{c_l}) \setminus \left\{ t_{X_i}, \frac{t_{X_i}x_{c_l}}{c_l} \right\} \subset \partial\mathcal{O} .$$

Now, both $t_{X_i}, \frac{t_{X_i}x_{c_l}}{c_l}$ cannot be in $\partial\mathcal{O}$ without contradicting the lemma 3.5. Similarly, it can be argued that if \overline{X}_i appears in C_l then both $t_{\overline{X}_i}$ and $\frac{t_{\overline{X}_i}x_{c_l}}{c_l}$ cannot be in $\partial\mathcal{O}$. \square

3.3. Correctness of reduction. We now state the main theorem of this paper.

Theorem 3.13. *3,4-SAT instance \mathcal{I} is satisfiable if and only if \mathcal{F} is a \mathcal{O} -border basis with respect to some order ideal \mathcal{O} .*

Proof. Suppose \mathcal{F} is an \mathcal{O} -border basis of \mathfrak{a} with respect to order ideal \mathcal{O} , we will construct an assignment to \mathcal{I} and show that it is a satisfying assignment.

The truth values to variables in instance \mathcal{I} are assigned as follows. Consider the polynomial $t_{X_i} + t_{\overline{X}_i} \in F_v$ for $i \in \{1, \dots, n\}$. Exactly one among the terms $t_{X_i}, t_{\overline{X}_i}$ has to be in \mathcal{O} and the other term in $\partial\mathcal{O}$. If t_{X_i} is in \mathcal{O} , then assign true value to variable X_i and if $t_{\overline{X}_i}$ is in \mathcal{O} , then assign false value to X_i .

Claim. The above assignment is a satisfiable assignment to \mathcal{I} .

Proof. Assume that the above assignment is not a satisfiable assignment then there exists a clause C_l for $l \in \{1, \dots, m\}$ such that C_l is not satisfied. Without loss of generality let C_l be of the form $(X_i \vee \overline{X}_j \vee X_k)$, where $i, j, k \in \{1, \dots, n\}$. Since C_l is not satisfied, all of $t_{X_i}, t_{\overline{X}_j}, t_{X_k}$ are in $\partial\mathcal{O}$. From Corollary 3.12, this implies that $\frac{t_{X_i}x_{c_l}}{c_l}, \frac{t_{\overline{X}_j}x_{c_l}}{c_l}, \frac{t_{X_k}x_{c_l}}{c_l} \in \mathcal{O}$. Consider the polynomial

$$f = \frac{t_{X_i}x_{c_l}}{c_l} + \frac{t_{\overline{X}_j}x_{c_l}}{c_l} + \frac{t_{X_k}x_{c_l}}{c_l} \in F_c .$$

All the terms in the support of f are in \mathcal{O} . But this is not possible since \mathcal{F} is a border basis and f should contain exactly one term in $\partial\mathcal{O}$, a contradiction.

Suppose that \mathcal{I} is satisfiable. Let A be a satisfying assignment to instance \mathcal{I} . Using A , we will construct an order ideal \mathcal{O} such that \mathcal{F} is a \mathcal{O} -border basis. For that we first construct sets \mathcal{O} and T and prove the following statements.

- i) \mathcal{O} is an order ideal,
- ii) T is the border of the order ideal \mathcal{O} i.e. $T = \partial\mathcal{O}$,
- iii) \mathcal{F} is a \mathcal{O} -border prebasis and
- iv) \mathcal{F} is a \mathcal{O} -border basis.

We construct the set T as follows.

- 1) For $i \in \{1, \dots, n\}$, if X_i is assigned to be false in assignment A then include t_{X_i} in T . If X_i is assigned to be true then include $t_{\overline{X}_i}$ in T
- 2) Let C_l be a clause in instance \mathcal{I} for $l \in \{1, \dots, m\}$. Assume that $C_l = (X_i \vee \overline{X}_j \vee X_k)$ for $i, j, k \in \{1, \dots, n\}$. Associated to this clause, we have the polynomial

$$f = \frac{t_{X_i}x_{c_l}}{c_l} + \frac{t_{\overline{X}_j}x_{c_l}}{c_l} + \frac{t_{X_k}x_{c_l}}{c_l} \in \mathcal{F}.$$

If one term among $t_{X_i}, t_{\overline{X}_j}, t_{X_k}$, say t_{X_i} , is not in T (if there are more than one term among $t_{X_i}, t_{\overline{X}_j}, t_{X_k}$ not in T then pick one term arbitrarily) then include $\frac{t_{X_i}x_{c_l}}{c_l}$ in T . Thus, in the support of every clause polynomial no more than one term is included in T .

- 3) Include all the terms in the support of $F_1 \cup F_2$ to be in T .

Claim. Let $\mathcal{O} = \mathbb{T}_{\leq 8} \setminus T$. \mathcal{O} is an order ideal.

Proof. All the terms of total degree 8 are in T (by construction). Thus, \mathcal{O} contains terms of total degree 7 or less. If $t \in \mathcal{O}$ and $t'|t$ then $\deg(t') < \deg(t) \leq 7$ which implies that $\deg(t') < 7$. But since $T \subset \text{Supp}(\mathcal{F})$ and $\text{Supp}(\mathcal{F})$ contains no term of total degree less than 7, all the terms of total degree 6 or less are in \mathcal{O} . Therefore, $t' \in \mathcal{O}$.

Claim. T is the border of the order ideal \mathcal{O} i.e. $T = \partial\mathcal{O}$.

Proof. Let $t' \in \partial\mathcal{O}$. There exists a term $t \in \mathcal{O}$ and an indeterminate y such that $t' = ty$. Since all the terms in \mathcal{O} have total degree 7 or less, we have $\deg(t) \leq 7$ which implies that $t' = ty \in \mathbb{T}_{\leq 8}$. By our construction of \mathcal{O} , this means that $t' \in T$. This proves that $\partial\mathcal{O} \subset T$.

In order to show $T \subset \partial\mathcal{O}$, it is enough to show that for a term $t \in T$, there exists an indeterminate y such that $y|t$ and $\frac{t}{y} = t' \notin T$ i.e. $t' \in \mathcal{O}$. Now, since all the terms of total degree 6 or less are in \mathcal{O} , all the terms of total degree 7 in T are also in $\partial\mathcal{O}$. So, assume that there exists a term t such that $\deg(t) = 8$ and $k(t) \subset T$. We prove by contradiction that such a term cannot exist. Since all the terms of total degree 7 in T are in $\cup_{i=1}^n R_i$, $k(t) \subset \cup_{i=1}^n R_i$. From Lemma 3.4, $k(t)$ should be a subset of R_i for some $i \in \{1, \dots, n\}$. There are two cases for t as described below.

(i) $t \in P_i$: Assume without loss of generality, $t = t_{X_i}x_{c_l} \in P_{X_i}$ for $i \in \{1, \dots, n\}, l \in \{1, \dots, m\}$. By our construction, both t_{X_i} and $\frac{t_{X_i}x_{c_l}}{c_l}$ cannot be in T . Hence atleast one child of t is in \mathcal{O} and thus not all terms in $k(t)$ is contained in T . So, this case is not possible.

(ii) $t \notin P_i$: From Corollary 3.3, we have

$$\begin{aligned} |k(t) \cap R_i| &= |k(t)| \leq |(P_{X_i} \cup P_{\bar{X}_i})| \\ &\Rightarrow |k(t)| \leq |P_i| \\ &\Rightarrow |I(t)| \leq |P_i|. \end{aligned}$$

Now, for any term $t' \in k(t)$ we have $I(t') \leq |P_i|$. But from Lemma 3.6, $I(t'') \geq |P_i| + 2$ for any term $t'' \in k(P_i) = R_i$. Thus this case is not possible.

From the above two cases we get a contradiction that there exists a term t such that $k(t) \subset R_i$ for some $i \in \{1, \dots, n\}$ and thus $k(t) \not\subset T$. So, t has atleast one child in \mathcal{O} . Thus, $T \subset \partial\mathcal{O}$.

Claim. \mathcal{F} is a \mathcal{O} -border prebasis.

Proof. In order to show \mathcal{F} is a \mathcal{O} -border prebasis, we have to show that each polynomial in \mathcal{F} has exactly one term in $\partial\mathcal{O}$ and the rest of the terms in \mathcal{O} . We show this for all the polynomials in \mathcal{F} :

- t -polynomials: From our construction, all the terms in the t -polynomials are in T i.e. in $\partial\mathcal{O}$ and hence each polynomial has exactly one term in $\partial\mathcal{O}$.
- v -polynomials: Again by our construction, each v -polynomial has exactly one term in T i.e. $\partial\mathcal{O}$ and the other term in \mathcal{O} .
- c -polynomials: Consider a clause C_l for $l \in \{1, \dots, m\}$. Assume that $C_l = (X_i \vee \bar{X}_j \vee X_k)$ where $i, j, k \in \{1, \dots, n\}$ in the instance \mathcal{I} . Let f be the polynomial associated with the clause C_l :

$$f = \frac{t_{X_i}x_{c_l}}{c_l} + \frac{t_{\bar{X}_j}x_{c_l}}{c_l} + \frac{t_{X_k}x_{c_l}}{c_l} \in \mathcal{F}.$$

Since all the terms in the support of f have total degree 7, the terms must either be in $\partial\mathcal{O}$ or \mathcal{O} . Consider the following cases:
Case (i): More than one term in f is in $\partial\mathcal{O}$: this cannot happen from our construction.

Case (ii): All the terms are in \mathcal{O} : This can happen only if all of $t_{X_i}, t_{\bar{X}_j}, t_{X_k}$ are in $\partial\mathcal{O}$ which implies that X_i, \bar{X}_j, X_k are false in assignment A . So, C_l is false. But this is not possible since assignment A satisfies instance \mathcal{I} . Hence this case is not possible.

From the above two cases, we deduce that exactly one term in

the support of f belongs to $\partial\mathcal{O}$ and from our construction, rest of the terms in f must belong to \mathcal{O} .

Since any polynomial in \mathcal{F} must be either a t -polynomial, c -polynomial or v -polynomial, from the above argument we deduce that \mathcal{F} is a \mathcal{O} -border prebasis.

Claim. \mathcal{F} is a \mathcal{O} -border basis of \mathfrak{a} .

Proof. Since \mathcal{F} is a \mathcal{O} -border prebasis, if \mathcal{F} satisfies Buchberger criterion for border basis then \mathcal{F} is a \mathcal{O} -border basis. Thus we need to show that for any two neighbouring polynomials $f, g \in \mathcal{F}$, $S(f, g)$ can be written as a linear combination of polynomials in \mathcal{F} . Before we consider the following cases for f and g we note that any polynomial containing only terms of total degree 8 in its support can be expressed as a sum of t -polynomials in $F_1 \subset \mathcal{F}$. Thus, in order to prove that \mathcal{F} satisfies Buchberger criterion it is enough to show that the support of $S(f, g)$ contains only terms of total degree 8. Neighbouring polynomials f, g can be of the following cases,

Case (i): f and g are t -polynomials: then $S(f, g) = 0$.

Case (ii): f is a t -polynomial and g is a c -polynomial or a v -polynomial: All the terms in $\text{Supp}(g)$ have total degree 7. Hence for any indeterminate y , all the terms in $\text{Supp}(yg)$ are of total degree 8. If $f \in F_2$, then yf for any indeterminate y is also a t -polynomial of total degree 8. The S-polynomial of f and g can be

$$S(f, g) = f - y_1g$$

or

$$S(f, g) = y_2f - y_1g,$$

for some indeterminates y_1, y_2 . In the first case, f has to be in F_1 (if f were to be in F_2 , by the way we have written the S-polynomial the border term of total degree 7 in f is equal to y_1b of total degree 8 where b is the border term in g which is not possible) and hence support of $S(f, g)$ contains only terms of total degree 8. The second case can happen only if $f \in F_2$ and hence support of $S(f, g)$ contains only terms of total degree 8.

Case (iii): f and g are not t -polynomials: S-polynomial of f and g is of the form,

$$S(f, g) = y_1f - y_2g,$$

for some indeterminates y_1, y_2 . As argued before, all the terms in the support of y_1f and y_2g are of total degree 8. Hence, all the terms in the support of $S(f, g)$ contains only terms of total degree 8. From the

three cases it follows that \mathcal{F} is a \mathcal{O} -border basis of \mathfrak{a} . □

Thus, we have proved that I has a satisfying assignment if and only if \mathcal{F} is a \mathcal{O} -border basis of $\mathfrak{a} = \langle \mathcal{F} \rangle$ for some order ideal \mathcal{O} . There is a polynomial time reduction from 3,4-SAT instance to BBD instance and since 3,4-SAT is NP-complete, we have the result that BBD is NP-complete.

4. CONCLUSION

In this paper we introduced the Border Basis Detection and proved it to be NP-complete.

ACKNOWLEDGMENTS

Authors would like to thank Vikram M. Tankasali and Prashanth Puranik for their useful comments and suggestions on this work.

REFERENCES

- [1] W. Auzinger and H. J. Stetter. An elimination algorithm for the computation of all zeros of a system of multivariate polynomial equations. In *Numerical mathematics, Singapore 1988*, volume 86 of *Internat. Schriftenreihe Numer. Math.*, pages 11–30. Birkhäuser, Basel, 1988.
- [2] Gábor Braun and Sebastian Pokutta. Border bases and order ideals: a polyhedral characterization. *arXiv:0912.1502v2*, 2010.
- [3] Yufu Chen and Xiaohui Meng. Border bases of positive dimensional polynomial ideals. In *Proceedings of the 2007 international workshop on Symbolic-numeric computation*, SNC '07, pages 65–71, New York, NY, USA, 2007. ACM.
- [4] Peter Gritzmann and Bernd Sturmfels. Minkowski addition of polytopes: computational complexity and applications to gröbner bases. *SIAM J. Discret. Math.*, 6(2):246–269, 1993.
- [5] Achim Kehrein and Martin Kreuzer. Characterizations of border bases. *Journal of Pure and Applied Algebra*, 196:251–270, April 2005.
- [6] Achim Kehrein and Martin Kreuzer. Computing border bases. *Journal of Pure and Applied Algebra*, 205:279–295, May 2006.
- [7] Achim Kehrein, Martin Kreuzer, and Lorenzo Robbiano. An algebraists view on border bases. In *Solving Polynomial Equations*, volume 14 of *Algorithms and Computation in Mathematics*, pages 169–202. Springer Berlin Heidelberg, December 2005.
- [8] Bernard Mourrain. A new criterion for normal form algorithms. In *Lecture Notes In Computer Science; Vol. 1719*, pages 430 – 443. Springer-Verlag, London, UK, 1999.
- [9] B. Sturmfels and M. Wiegmann. Structural Gröbner basis detection. *Applicable Algebra in Engineering, Communication and Computing*, 8(4):257–263, 1997.
- [10] C.A. Tovey. A simplified NP-complete satisfiability problem. *Discrete Applied Mathematics*, 8(1):85–89, 1984.

DEPT. OF COMPUTER SCIENCE AND AUTOMATION, INDIAN INSTITUTE OF
SCIENCE

E-mail address: `prabhanjan@csa.iisc.ernet.in`

DEPT. OF COMPUTER SCIENCE AND AUTOMATION, INDIAN INSTITUTE OF
SCIENCE

E-mail address: `ambedkar@csa.iisc.ernet.in`